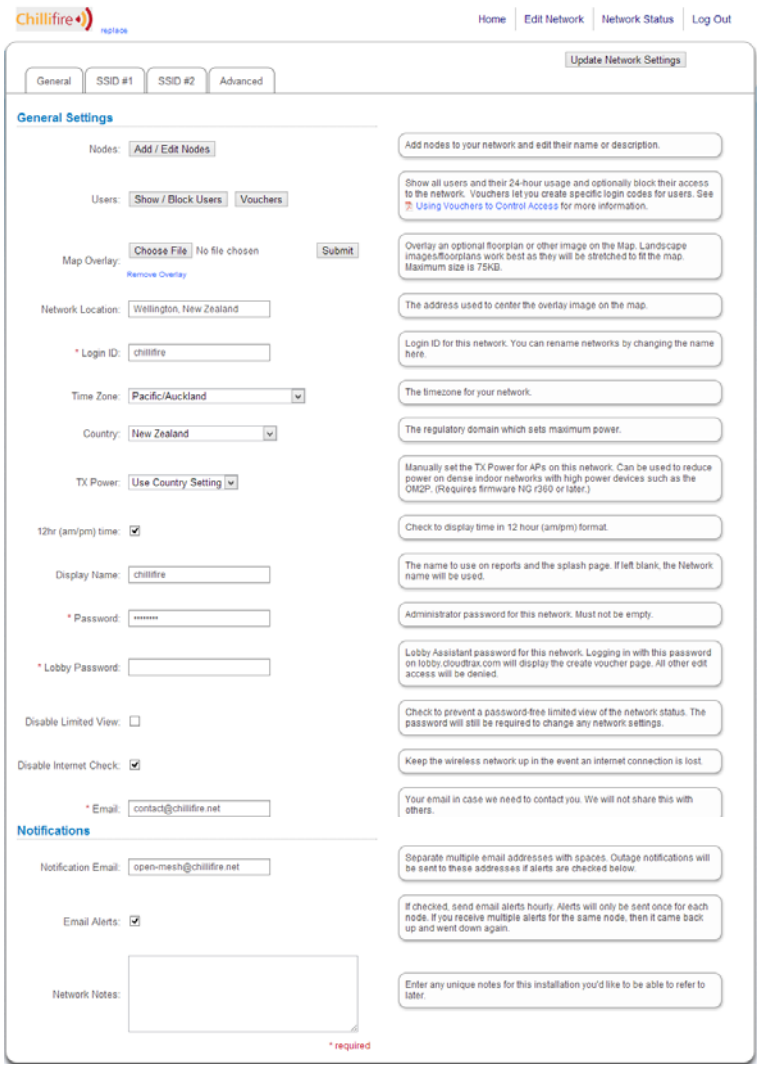
This guide is valid for Open-Mesh / Cloudtrax using firmware-ng or robin-mesh firmware

To integrate Chillifire Hotspots with Open-Mesh networks first of all you have to have an account their mesh network control panel on https://www.cloudtrax.com as much as you need an account with Chillifire. You can create a free Chillifire account on http://www.chillifire.net .

There is nothing special to consider in the setup of the Chillifire account, which you can configure any way you like to, free, pay-per-use, voucher based, online-payment, your own logo, colour scheme etc. However, the open-mesh/cloudtrax account has to be setup in a certain way to work with your Chillifire account:

General Tab

There is nothing much to consider on this tab although we recommend to un-check 'Disable Limited View' and to check 'Disable Internet Check'. We also recommend you set the 'TX Power' field to 'Use Country Settings' to avoid any issues within your regulatory jurisdiction. Other than that just enter your relevant contact details on this screen and press 'Update Network Settings' at the top of the screen.



SSID #1 Tab

This screen sets up your mesh network's connection to the hotspot system, and thus is the centre point of your setup:

Make sure the 'Hide' field is NOT checked, so potential customers can find the hotspot.

We recommend you the same SSID for all mesh network nodes, so your users can roam between routers. To enable this put your hotspots name into the 'Network Name' field and un-check the 'Use Node Name' field. The 'Network Name' must be less than 32 characters and should not contain any characters other than letters, number, spaces, underscores and dashes.

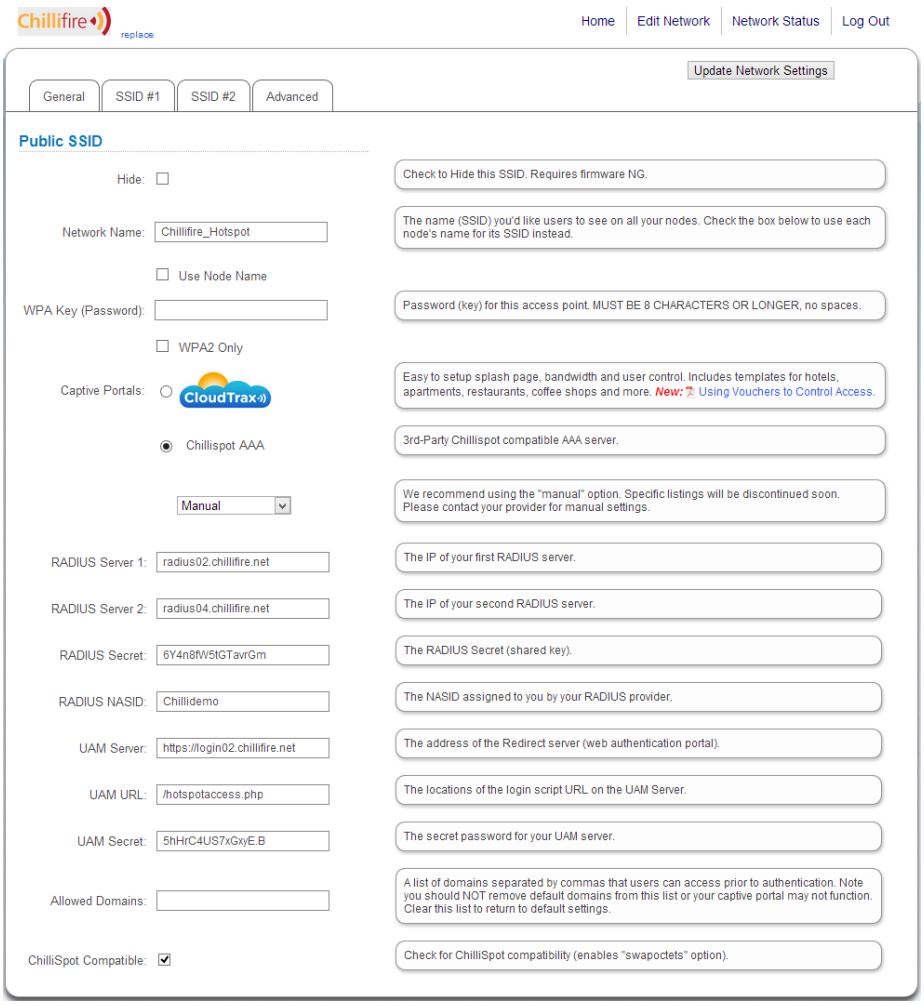
Do not set a 'WPA Key' and do not check the 'WPA2 Only' field.

Choose 'Chillispot AAA' and select 'Manual' settings.

Select the 'RADIUS Server 1' setting according to you location. Choose 'radius 06.chillifire.net' if you are located in the Americas, 'radius04.chillifire.net' if you are located in the Europe, Africa and the Near East, and 'radius 02.chillifire.net' if you are located in the Australasia. Choose a different location's radius server for the 'RADIUS Server 2'.

'RADIUS Secret' must be set to '6Y4n8fW5tGTavrGm'.

'RADIUS NASID' must be set to the name of your Chillifire account (Chillidemo in this example).



For the ‘UAM Server’ again choose the right server for your locality for best performance: ‘https://login06.chillifire.net’ if you are located in the Americas, ‘https://login04.chillifire.net’ if you are located in the Europe, Africa and the Near East, and ‘https://login02.chillifire.net’ if you are located in the Australasia.

‘UAM URL’ must be set to ‘/hotspotaccess.php’.

‘UAM Secret’ must be set to ‘5hHrC4US7xGxyE.B’.

You can leave ‘Allowed Domains’ blank if you do NOT intend to sell hotspot acces only. In that case only add domains to the field, separated by commas, for such domains that you want users to have access without needing to login on to the hotspot. This could be promotional pages or your business homepage to give but some examples. IF you DO intend to sell hotspot access online you MUST add the following string to the allowed domain field:

paypal.com,paypalobjects.com,paypal-metrics.com,112.2o7.net,moneybookers.com,skrill.com,omtdrc.net,verisign.com,amadesa.com,2checkout.com,thawte.com,securecode.com,adyen.com,paysafecard.com,mycardsecure.com,mixpanel.com,payfast.co.za,hittail.com,mbsvr.net,
mxpnl.com,chillifire.net,secure5.arcot.com,cap.securecode.com,seal.verisign.com,seal.entrust.net,i1.mbsvr.net,api.recaptcha.net,paypalssl.doubleclick.net,mp.apmebf.com,altfarm.mediaplex.com,images.scanalert.com,seal.godaddy.com

Note: If you cut and paste the content from this PDF document please make sure that line breaks are removed.

The field ‘ChilliSpot Compatible’ must be checked.

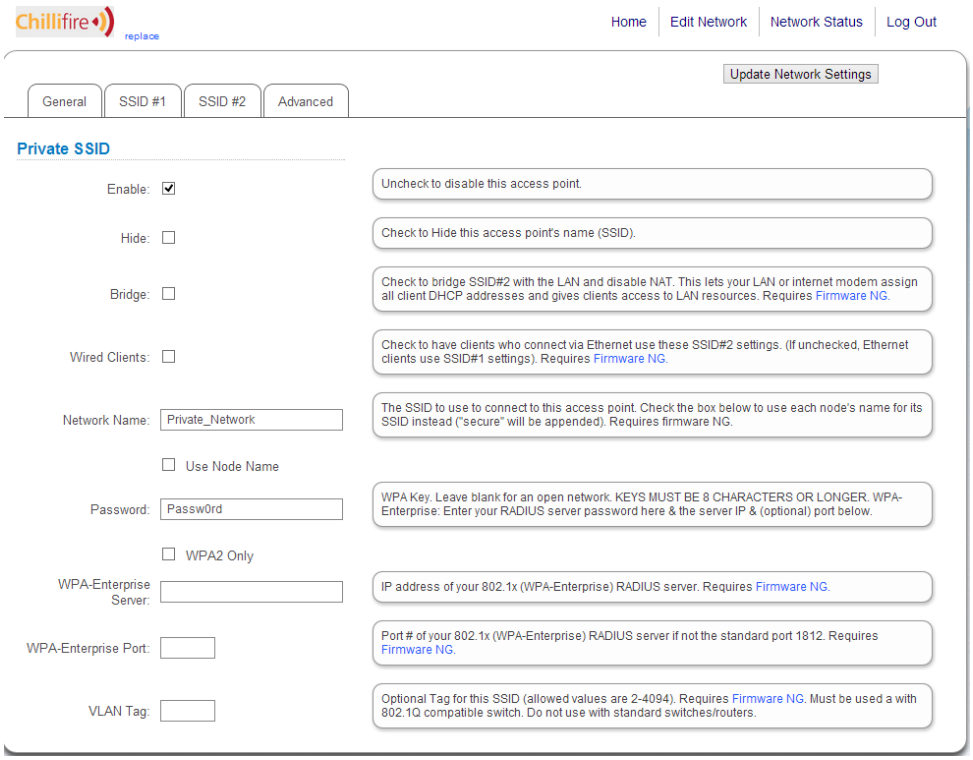
Save settings by clicking on press ‘Update Network Settings’ at the top of the screen.

SSID #2 Tab

Only enable this second SSID, if you want to offer a free access to the Internet, which bypasses the Hotspot, but requires a pre-shared key (PSK), i.e. a password.

If you enable this feature make sure the fields 'Bridge' is not checked.

If you want the Ethernet jack on the OM2P or other devices with more than one Ethernet jack to be hotspot controlled then make sure 'Wired Clients' is not checked. If you do check the and 'Wired Clients' field the Ethernet jack will bypass the hotspot and gain any device connected to it free access to the Internet.

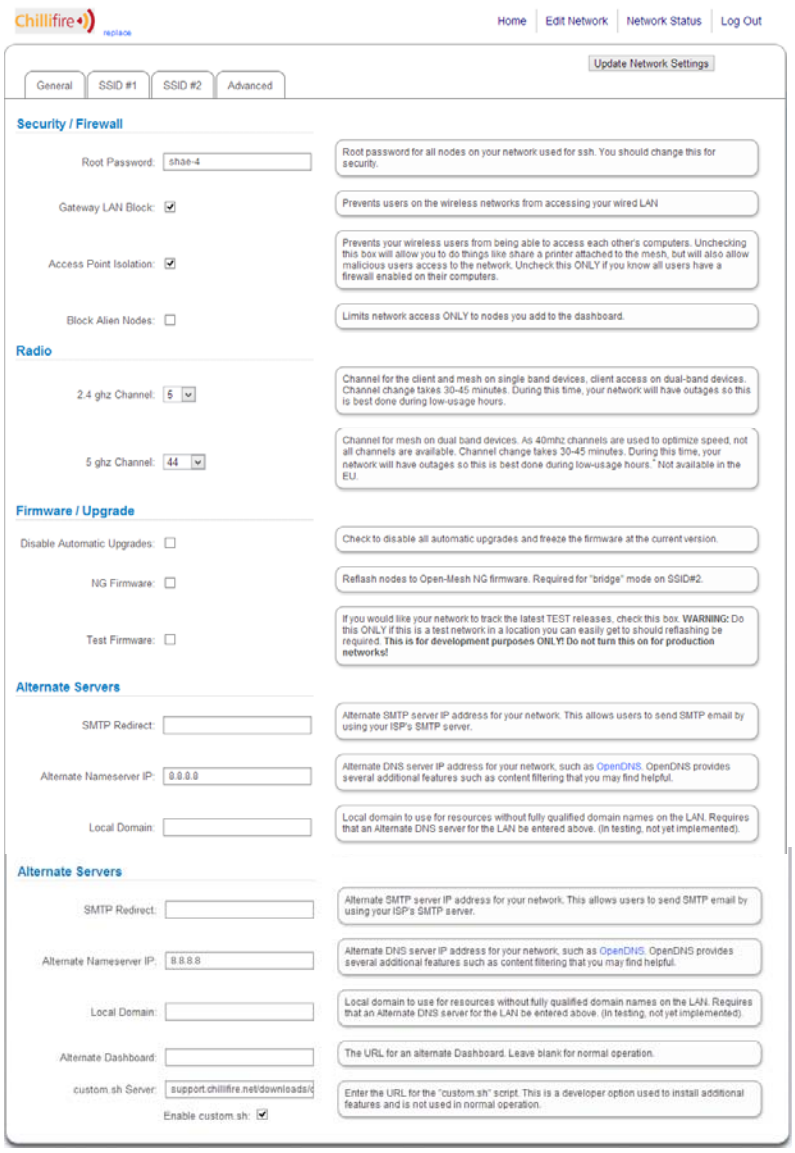


You must give this non-Hotspot network a name (Private_Network in this example) and set a Password (Passw0rd in this example).

Leave 'WPA Only' and all other fields on this page unchecked and empty.

Save settings by clicking on press 'Update Network Settings' at the top of the screen.

Advanced Tab



Set 'Root Password' to a secure password known only to you.

'Gateway LAN Block', 'Access Point Isolation', and 'Block Alien Nodes' must all be set.

Leave the channels unchanged, unless you have a lot of interference for other Wi-Fi routers on the same or on close channels.

'Disable Automatic Upgrades', 'NG firmware', and 'Test Firmware' should be unchecked unless you are an advanced open-mesh user and know what you are doing.

'SMTP Redirect' is useful to populate with your ISP's own SMTP server's IP address.

'Alternate Nameserver IP' can either be 8.8.8.8 for Google DNS, or alternatively you can link a service like Open DNS, or simply link you ISP's own DNS server for fast performance.

Leave 'Local Domain' and 'Alternate Dashboard' blank.

The most important setting on this page is the 'custom.sh Server' which MUST be set to 'support.chillifire.net/downloads/openmesh/'

'Enable custom.sh' MUST be checked.

Save settings by clicking on press 'Update Network Settings' at the top of the screen.

Adding Mesh Nodes to the Network

You'll be taken to the General Settings tab of the Edit Network page. On the top of the "Edit Network" page is an "Add/Edit Nodes" button. Click it.

A Google map, centred on the address you entered when you created the network, will appear in a popup. You can often (depending on location) click the "Satellite" view button and zoom in for a closer look. Click the map where you want to add your first node.

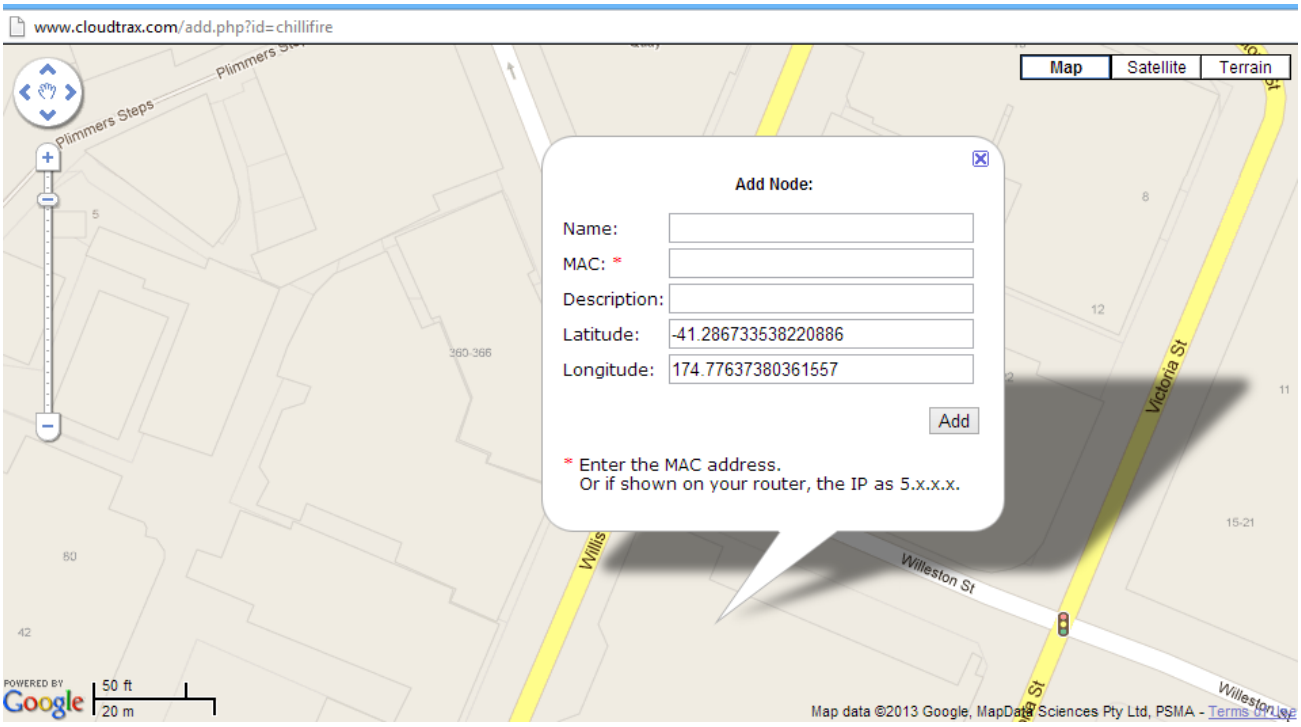
Next, you'll see a dialogue similar to the one on the right. Fill in the following information:

Name: Enter a name for this node. This name is used to reference its location and will be displayed in reports. It does not affect users.

MAC address: A MAC address is a sequence of 12 numbers and the letters A-F often separated by colons (e.g. 00:02:6F:8A:B2:6E). This can be found on a label on the bottom of the router and on the side of the product box. For the MR500, there are 3 MAC addresses shown, and you want to enter the one on the top, listed as the "WAN MAC."

Description: You can enter optional descriptive text that will be shown on the reports. This is typically used to keep notes on where the node is installed, etc.

Click "Add" and repeat the process for each additional node.



Installing the Nodes

Once your nodes are added to CloudTrax, it's time to install them.

First, connect your Gateway unit to the Internet with an Ethernet cable. This can be plugged in directly to your high-speed modem (if it has a single Ethernet port, power cycle it first), or it can be fed from a router or switch. If it can get an Internet connection through the cable, it'll connect to CloudTrax. Once the Ethernet cable is plugged in, connect power.

Next, plug in additional nodes as either gateways (connected to Ethernet) or repeaters, connected only to power.

To ensure strong, consistent signal coverage, follow these guidelines:

1. Place your gateway in the centre of the network. For most devices, every time data is transmitted over one repeater hop, it loses half its speed. A central gateway minimizes the number of hops required.

2. Never go through more than three walls or floors.

3. Never go more than 50-150 feet (depending on building materials) between nodes.

4. Install no more than about five repeaters to every one gateway.

Once all nodes are plugged in, you should see them turn green on the CloudTrax Network Status page in about 5 to 15 minutes.

Allow some 20 minutes; after that time you should see the routes in the Chillifire Control panel's Router Status screen. The system automatically registers all mesh nodes against the account or sub-account you entered in the NASID field on the SSID #1 tab.